RECEIVED
CENTRAL FAX CENTER
JAN 16 2007

Amendment to the Claims

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for generating a control message to be transmitted from a first network device to a second network device in a data network, the control message relating to an action to be performed at the second network device, the method comprising:

determining a first control message to be generated, wherein the first control message corresponds to a security protocol control message;

identifying reason information relating to at least one reason for generating the first control message; and

generating the first control message, wherein the first control message includes explicit reason information relating to the identified at least one reason for generating the control message;

wherein the reason information includes at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

wherein the first control message includes a first payload selected from a group consisting of: a security association payload and a delete payload;

wherein the first payload includes the reason information.

2. (previously presented) The method of claim 1 wherein the first control message is formatted in accordance with an Internet Key Exchange protocol.

3. (cancelled).

4. (previously presented) The method of claim 1 wherein the first control message is formatted in accordance with an Internet Security Association Key Management Protocol.

5. (original) The method of claim 1 wherein the first control message corresponds to a control message used for modifying a security association.

6. (original) The method of claim 1 further comprising transmitting the first control message to the second network device to thereby cause the second network device to implement an appropriate action in response to the first control message.

7. (currently amended) A method for communicating between nodes in a data network, the method comprising:

receiving a first control message from a first node, the first control message corresponding to a security protocol control message, the first control message including explicit reason information relating to at least one reason for the generation of the first control message, the first control message including a first payload, the reason information being included in the first payload, the first payload being selected from a group consisting of: a security association payload and a delete payload, the reason information including at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

identifying the reason information;

determining an appropriate response to the first control message using at least said reason information; and

implementing said appropriate response.

8. (previously presented) The method of claim 7 wherein the first control message is formatted in accordance with an Internet Key Exchange protocol.

9. (cancelled).

10. (previously presented) The method of claim 7 wherein the first control message is formatted in accordance with an Internet Security Association Key Management Protocol.

11. (original) The method of claim 7 wherein the first control message corresponds to a control message used for modifying a security association.

12. (original) The method of claim 7 further comprising:

implementing a first response to the first control message if the reason information includes a first reason code; and

implementing a second response to the control message if the reason information includes a second reason code.

13. (original) The method of claim 7 wherein the control message relates to an action to be performed at a network device receiving the control message.

14. (currently amended) A computer program product for generating a control message to be transmitted from a first network device to a second network device in a data network, the control message relating to an action to be performed at the second network device, the computer program product comprising:

a computer usable medium having computer readable code embodied therein, the computer readable code comprising:

computer code for determining a first control message to be generated, wherein the first control message corresponds to a security protocol control message;

computer code for identifying reason information relating to at least one reason for generating the first control message; and

computer code for generating the first control message, wherein the first control message includes explicit reason information relating to the identified at least one reason for generating the control message;

wherein the reason information includes at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

wherein the first control message includes a first payload selected from a group consisting of: a security association payload and a delete payload;

wherein the first payload includes the reason information.

15. (previously presented) The computer program product of claim 14 is formatted in accordance with an Internet Key Exchange protocol.

16. (cancelled).

17. (previously presented) The computer program product of claim 14 wherein the first control message is formatted in accordance with an Internet Security Association Key Management Protocol.

18. (original) The computer program product of claim 14 wherein the first control message corresponds to a control message used for modifying a security association.

19. (currently amended) A computer program product for communicating between nodes in a data network, the computer program product comprising:

a computer usable medium having computer readable code embodied therein, the computer readable code comprising:

computer code for receiving a first control message from a first node, the first control message corresponding to a security protocol control message, the first control message including explicit reason information relating to at least one reason for the generation of the first control message, the first control message including a first payload, the first payload including the reason information, the first payload being selected from a group consisting of: a security association payload and a delete payload;

computer code for identifying the reason information, the reason information including at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

computer code for determining an appropriate response to the first control message using at least said reason information; and

computer code for implementing said appropriate response.

20. (previously presented) The computer program product of claim 19 wherein the first control message is formatted in accordance with an Internet Key Exchange protocol.

21. (cancelled).

22. (previously presented) The computer program product of claim 19 wherein the first control message is formatted in accordance with an Internet Security Association Key Management Protocol.

23. (original) The computer program product of claim 19 wherein the first control message corresponds to a control message used for modifying a security association.

24. (original) The computer program product of claim 19 further comprising:

computer code for implementing a first response to the first control message if the reason information includes a first reason code; and

computer code for implementing a second response to the control message if the reason information includes a second reason code.

25. (original) The computer program product of claim 19 wherein the control message relates to an action to be performed at a network device receiving the control message.

26. (currently amended) A system for communicating between nodes in a data network, the system comprising:

means for receiving a first control message from a first node, the first control message corresponding to a security protocol control message, the first control message including explicit reason information relating to at least one reason for the generation of the first control message, the reason information including at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

means for identifying the reason information;

means for determining an appropriate response to the first control message using at least said reason information; and

means for implementing said appropriate response;

wherein the first control message includes a first payload selected from a group consisting of: a security association payload and a delete payload;

wherein the first payload includes the reason information.

27. (previously presented) The system of claim 26 wherein the first control message is formatted in accordance with an Internet Key Exchange protocol.

28. (cancelled).

29. (previously presented) The system of claim 26 wherein the first control message is formatted in accordance with an Internet Security Association Key Management Protocol.

30. (original) The system of claim 26 wherein the first control message corresponds to a control message used for modifying a security association.

31. (original) The system of claim 26 further comprising means for transmitting the first control message to the second network device to thereby cause the second network device to implement an appropriate action in response to the first control message.

32. (original) The system of claim 26 further comprising:

means for implementing a first response to the first control message if the reason information includes a first reason code; and

means for implementing a second response to the control message if the reason information includes a second reason code.

33. (original) The system of claim 26 wherein the control message relates to an action to be performed at a network device receiving the control message.

34. (currently amended) A system for generating a control message to be transmitted to a network device in a data network, the control message relating to an action to be performed at the network device, the system comprising:

at least one CPU;

memory; and

at least one interface for communicating with the network device;

the system being configured or designed to determine a first control message to be generated, wherein the first control message corresponds to a security protocol control message;

the system being further configured or designed to identify reason information relating to at least one reason for generating the first control message; and

the system being further configured or designed to generate the first control message, wherein the first control message includes explicit reason information relating to the identified at least one reason for generating the control message;

wherein the reason information includes at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

wherein the first control message includes a first payload selected from a group consisting of: a security association payload and a delete payload;

wherein the first payload includes the reason information.

35. (previously presented) The system of claim 34 wherein the first control message is formatted in accordance with an Internet Key Exchange protocol.

36. (cancelled).

37. (previously presented) The system of claim 34 wherein the first control message is formatted in accordance with an Internet Security Association Key Management Protocol.

38. (original) The system of claim 34 wherein the first control message corresponds to a control message used for modifying a security association.

39. (original) The system of claim 34 being further configured or designed to transmit the first control message to a second network device to thereby cause the second network device to implement an appropriate action in response to the first control message.

40. (currently amended) A system for communicating between nodes in a data network, the system comprising:

at least one CPU;

memory; and

at least one interface for communicating with at least one network device, wherein the first control message corresponds to a security protocol control message;

the system being configured or designed to receive a first control message from a first node, the first control message corresponding to a security protocol control message, the first control message including explicit reason information relating to at least one reason for the generation of the first control message, the first control message including a first payload, the first payload including the reason information, the first payload being selected from a group consisting of: a security association payload and a delete payload, wherein the first payload includes the reason information, the reason information including at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

the system being further configured or designed to identify the reason information;

the system being further configured or designed to determine an appropriate response to the first control message using at least said reason information; and

the system being further configured or designed to implement said appropriate response.

41. (previously presented) The system of claim 40 wherein the first control message is formatted in accordance with an Internet Key Exchange protocol.

42. (cancelled).

43. (previously presented) The system of claim 40 wherein the first control message is formatted in accordance with an Internet Security Association Key Management Protocol.

44. (original) The system of claim 40 wherein the first control message corresponds to a control message used for modifying a security association.

45. (original) The system of claim 40 further comprising:

the system being further configured or designed to implement a first response to the first control message if the reason information includes a first reason code; and

the system being further configured or designed to implement a second response to the control message if the reason information includes a second reason code.

46. (previously presented) The method of claim 1:

wherein the security association payload is adapted to facilitate negotiation of a security association between a first network node and a second network node; and

wherein the delete payload is adapted to facilitate deletion of a security association associated with a first network node and a second network node.

47. (previously presented) The method of claim 7:

wherein the security association payload is adapted to facilitate negotiation of a security association between a first network node and a second network node; and

wherein the delete payload is adapted to facilitate deletion of a security association associated with a first network node and a second network node.

48. (previously presented) The computer program product of claim 14:

wherein the security association payload is adapted to facilitate negotiation of a security association between a first network node and a second network node; and

wherein the delete payload is adapted to facilitate deletion of a security association associated with a first network node and a second network node.

49. (previously presented) The computer program product of claim 19:

wherein the security association payload is adapted to facilitate negotiation of a security association between a first network node and a second network node; and

wherein the delete payload is adapted to facilitate deletion of a security association associated with a first network node and a second network node.

50. (previously presented) The system of claim 26:

wherein the security association payload is adapted to facilitate negotiation of a security association between a first network node and a second network node; and

wherein the delete payload is adapted to facilitate deletion of a security association associated with a first network node and a second network node.

51. (previously presented) The system of claim 34:

wherein the security association payload is adapted to facilitate negotiation of a security association between a first network node and a second network node; and

wherein the delete payload is adapted to facilitate deletion of a security association associated with a first network node and a second network node.

52. (previously presented) The system of claim 40:

wherein the security association payload is adapted to facilitate negotiation of a security association between a first network node and a second network node; and

wherein the delete payload is adapted to facilitate deletion of a security association associated with a first network node and a second network node.

53. (new) A method for generating a control message to be transmitted from a first network device to a second network device in a data network, the control message relating to an action to be performed at the second network device, the method comprising:

determining a first control message to be generated, wherein the first control message corresponds to a security protocol control message;

identifying reason information relating to at least one reason for generating the first control message; and

generating the first control message, wherein the first control message includes explicit reason information relating to the identified at least one reason for generating the control message;

wherein the reason information includes at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

wherein the first control message includes a first payload which includes the reason information.

54. (new) A system for generating a control message to be transmitted to a network device in a data network, the control message relating to an action to be performed at the network device, the system comprising:

at least one CPU;

memory; and

at least one interface for communicating with the network device;

the system being configured or designed to determine a first control message to be generated, wherein the first control message corresponds to a security protocol control message;

the system being further configured or designed to identify reason information relating to at least one reason for generating the first control message; and

the system being further configured or designed to generate the first control message, wherein the first control message includes explicit reason information relating to the identified at least one reason for generating the control message;

wherein the reason information includes at least one reason selected from a group of reasons consisting of: a user initiated reason, an expired lifetime reason, and a no error reason;

wherein the first control message includes a first payload which includes the reason information.